



ICSJWG Newsletter

ICSJWG 2010 Spring Conference

The ICSJWG 2010 Spring Conference was a success, as over 300 industry-wide participants came together for the three day conference held in San Antonio, from April 5-8. The conference provided participants with a chance to engage in discussions about security controls, network with others in the industry, and learn about the latest control systems security issues. The three-day conference activities included a day devoted to subgroup meetings, a day of presentations given by industry leaders in control systems cyber security, which focused on three tracks: technology, case studies, and policy and standards, and a day dedicated to the *Introduction to Industrial Control Systems Cybersecurity training course*.

Presentations from the conference are available on the ICSJWG website: http://www.us-cert.gov/control_systems/icsjwg/presentations.html.

ICSJWG Subgroups

The ICSJWG Subgroups have worked diligently on their goal, objectives and milestones since the last conference. Below is an update on the progress of each subgroup.

Information Sharing Subgroup

Co-Chairs: George Bamford and Nathan Faith

The ICSJWG has identified HSIN as the collaboration tool to facilitate information sharing amongst the control systems community. The real work is providing content and data and making it relevant to the users. The group needs help from industry to identify thresholds for the information and reporting standards as it goes to ICS-CERT. Contact one of the subgroup co-chairs or liaisons at icsjwg@dhs.gov so that they can implement and incorporate your data to put it to use for the community.

International Subgroup

Co-Chairs: Seán McGurk and Michael Assante

The International Subgroup has begun work on the first milestone from the charter being led by Art Manion. DHS needs active participants, and especially international stakeholders to become involved with the subgroup activities. The geographic separation of subgroup members presents a challenge to

About the ICSJWG

The ICSJWG is a collaborative and coordinating body operating under the Critical Infrastructure Partnership Advisory Council (CIPAC) requirements. The ICSJWG provides a vehicle for communicating and partnering across all critical infrastructure and key resources (CIKR) sectors between federal agencies and departments as well as private asset owner/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the facilitation and collaboration of the industrial control systems stakeholder community in securing CIKR by accelerating the design, development, and deployment of secure industrial control systems.

*For more information, visit
http://www.us-cert.gov/control_systems/icsjwg/*

the development of work plans and a hindrance to the setting of convenient meeting times. The adoption of the collaboration tool should alleviate this as the subgroup works through this key issue.

The intent of the subgroup is not to travel internationally. DHS does not sponsor travel to other countries.

Research and Development Subgroup

Co-Chairs: Dr. Douglas Maughan (Douglas.Maughan@dhs.gov) and David L Norton (DNORTO1@entergy.com).

The Research and Development subgroup is still actively seeking increased participation from industry stakeholders. This participation is critical for meeting the subgroup's objectives going forward.

Roadmap to Secure Industrial Control Systems

Co-Chairs: Perry Pederson (perry.pederson@nrc.gov) and Tim Roxey (Tim.Roxey@nerc.net).

The Roadmap subgroup drafted a Roadmap to improve control systems security across all sectors. The subgroup drew upon existing sector-specific roadmaps, such as that of the Energy sector, to guide the creation of this cross-sector roadmap. The Roadmap subgroup is also actively seeking increased participation from stakeholders across all sectors. Extensive participation is the key to making the cross-sector roadmap work.

Vendor Subgroup

Co-Chairs: Rick Lichtenfels (cssp@dhs.gov) and Eric Cosman (ECCosman@dow.com).

The Vendor subgroup focused on identifying its role and its relationship to the other subgroups as well as considering revising its objectives. The name "Vendor subgroup" implied that it was for vendors only. That is not its intent; the objective is much broader and includes collaboration with standards and technology developers, how to handle risk management, and other control systems issues within the vendor community. Participation is not limited to vendors, and the group is reaching out to other stakeholders. There are only two owner/operators currently participating in the group – this is an opportunity for more end users to consider getting involved.

Workforce Development Subgroup

Co-Chairs: Ben Wible (wibleb@ndu.edu), Dr. John Saunders (saunders@ndu.edu), and Marcus Sachs (marcus.sachs@verizon.com).

The Workforce Development subgroup completed Objective 1, Goal 1, of its charter: to identify existing ICS training programs. The co-chairs completed the initial research of available curricula and distributed copies to the participants at the conference. From there, they plan to do a feasibility study and identify gaps. Although the workforce development subgroup has members from many different backgrounds, they do not have many end users in the group. They would like participation from sector organizations and people with curriculum and training backgrounds. Please contact the co-chairs directly or ICSJWG@dhs.gov if interested in joining this subgroup.

Homeland Security Information Network (HSIN)

The ICSJWG will use the Homeland Security Information Network (HSIN) to facilitate collaboration among the subgroups. HSIN is a fully functional real-time collaboration portal with capabilities for

group calendars, document sharing, live chat rooms, and white board functionality. HSIN is not only for sharing of vulnerability and threat information; HSIN is a workroom for all the subgroups. Its Adobe Connect feature allows users to collaborate in real time. The HSIN ICSJWG portal will be located off of the HSIN CS Critical Sector homepage. There will be sub-portals for each of the ICSJWG subgroups. Each subgroup will be equipped with its own calendar and document collaboration sections. The ICSJWG HSIN portal under development and will be available within the next 60 days.

- If you need an HSIN account:
 - **Federal Employees:** Any federal employee who would like an HSIN ICSJWG account must be vetted and granted access through the HSIN-CS/ICSJWG portal administrators: Sunny Browarny (NCSD) and Adam Zoller (I&A) at ICSJWG@dhs.gov.
 - **Private Sector Partners:** Any private sector partner who would like access to HSIN must be vetted through their respective sector administrator (i.e. electrical sector partners obtain accounts through the electric sector administrator).
- If you already have an HSIN account, please provide your name, HSIN user name, ICSJWG subgroup affiliation, and critical infrastructure sector to ICSJWG@dhs.gov so we can provide you with access to the HSIN ICSJWG portal once it becomes available.

Save the Date – Fall Conference

The ICSJWG Fall Conference is tentatively scheduled for late October/early November. We will keep you posted when we have the exact date and location. If you have any venue ideas, please share them with us at icsjwg@dhs.gov!

Participation is Key!

Your participation and input is **critical** to the success of these subgroups and to the overall mission of ICSJWG to coordinate cybersecurity efforts to secure ICS across the nation's critical infrastructure. Please email the co-chairs or icsjwg@dhs.gov to get involved with one or more of the subgroups.

Advanced Training Events Scheduled for 2010

This event will provide intensive hands-on training on protecting and securing control systems from cyber attacks, including a very realistic Red Team / Blue Team exercise that will be conducted within an actual control systems environment. It will also provide an opportunity to network and collaborate with other colleagues involved in operating and protecting control systems networks.

The following advance training events have been scheduled for 2010:

- May 10-14, 2010 – International
- June 21-25, 2010 – International
- July 19-23 – Federal Partners
- Sept. 13-17 – US Asset Owners and Vendors

Additional offerings are still being planned and will be announced once dates are finalized. The training is held at the Control Systems Analysis Center located in Idaho Falls, Idaho and will provide intensive hands-on training on protecting and securing industrial control systems from cyber attacks, including a Red Team /Blue Team exercise that will be conducted within an actual control systems environment.

There is no cost to attend the training; however, travel expenses and accommodations are the responsibility of each participant. More information, including registration and future offerings, is available at: http://www.us-cert.gov/control_systems/

Conference Events Scheduled for 2010

The following is a listing of conferences and other events that the Control Systems Security Program (CSSP) is supporting and may be of interest to control system individuals involved in security.

- May 3-5, 2010 - **Intelligent Transportation Society 2010 Annual Meeting and Exposition**
 - <http://www.itsa.org/annualmeeting.html>
- June 13-18, 2010 - **22nd Annual FIRST Conference**
 - <http://conference.first.org/>
- June 14-16, 2010 - **Smart Electricity World USA 2010**
 - <http://www.terrapinn.com/2010/smartusa/>
- June 20-24, 2010 - **American Water Works Association ACE 10 Conference**
 - <http://www.awwa.org/>

Additional conferences will be announced once dates are finalized.

Contact Information

If you would like to contact the ICSJWG to ask a question or inquire about participation, please send an e-mail to icsjwg@dhs.gov.

The CSSP and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online reporting forms are available at <https://forms.us-cert.gov/report/>.

Other important contact information:

Web Site Address: http://www.us-cert.gov/control_systems/

ICS-CERT Email: ics-cert@dhs.gov

Phone: 1-877-776-7585

CSSP Email: cssp@dhs.gov